## REMARKS

Claims 35-55 are all the claims pending in the application. The independent claims are 35, 42, and 49. This Amendment amends claims 35, 42, and 49, and addresses each point of rejection raised by the Examiner. Favorable reconsideration is respectfully requested.

Applicants respectfully request acknowledgement of the drawing corrections submitted with the Amendment dated April 26, 2004 in the next Office action.

Claims 35, 37-42, 44-49, and 51-55 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,205,437 to Gifford ("Gifford") in view of U.S. Patent 6,327,578 to Linehan ("Linehan"). Claims 36, 43, and 50 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Gifford and Linehan, further in view of U.S. Publication No. 2001/0014158 to Baltzley ("Baltzley").

Applicants have amended independent claims 35, 42, and 49. No new matter is added.

The Examiner acknowledges that Gifford does not disclose sending a challenge request to the buyer over the network, but asserts that in view of the disclosures of Linehan, one of ordinary skill in the art would have been motivated to add such a feature to Gifford "because it provides security and verification means, thereby preventing fraud." Applicants respectfully submit that even if one of ordinary skill were to add a challenge request as disclosed by Linehan to the method of Gifford, the combination would still fail to suggest each limitation of the amended independent claims. For example, amended independent claim 35 recites:

> *in response to receiving an authentication request from a buyer over a network, the authentication request including a description of the payment transaction and an identity of a seller, sending a challenge request to the buyer over the network, the challenge request including a ~~message~~ summary of the payment transaction to be digitally signed by the buyer using a private key associated with the PKI key pair;*

The combination of Gifford and Linehan does not suggest this feature. In Gifford, a client computer requests a purchase by constructing "a payment order," adding an authenticator, and sending it for approval to a payment computer (*e.g.*, Gifford col. 8, lines 25-28). A payment order describes the identity of a sender, a payment amount, a beneficiary, and a sender unique nonce (Gifford col. 2, lines 59-61). A sender unique nonce is an identifier that is used only once

by a given sender (Gifford col. 2, lines 63-64). An example of sender unique nonces are unique timestamps (Gifford col. 2, lines 64-65).

A public-key cryptographic signature is used as the authenticator (*see* Gifford col. 10, lines 30-42). The payment order is verified by using the public key known to the payment computer (*see* Gifford col. 8, lines 28-31; col. 10, lines 40-42).

Linehan discloses that after a consumer's computer sends a start message to a merchant's computer, that the merchant replies with a merchant "initiation message" which includes a consumer's wallet initiation message, a merchant digital signature, and a digital certificate from an acquiring bank (*see* Linehan col. 4, lines 12-15). The wallet initiation message includes a payment amount, an order description, a timestamp, and a nonce (*see* Linehan col. 4, lines 15-17). The consumer's computer then sends over the internet some consumer identity and authentication information, such as userid and user password, plus the merchant message, to an issuer gateway (*see* Linehan col. 4, lines 19-23).

The issuer gateway then sends the consumer a challenge message (*see* Linehan col. 7, lines 26-27). The consumer's smart card then signs the challenge response (*see* Linehan col. 7, lines 30-33). The consumer's computer then combines the signed challenge response with the merchant's initiation message and sends it on to the issuer gateway (*see* Linehan col. 7, lines 33-35). The issuer gateway verifies the smart card's signature to verify the consumer's identify (*see* Linehan col. 7, lines 35-37).

There would be no motivation to combine the challenge response of Linehan with Gifford as Gifford teaches use of a nonce and a private key to encrypt the original payment order. The reason Linehan uses the challenge response is that the original request received from the user is not signed by the user, such that the challenge response is needed for verification. However, the nonce and signature of the original request in Gifford serves the same verification function, if not better, such that there would be no reason to repeatedly sign the same information.

Moreover, the challenge response of Linehan still does not suggest having the buyer sign a summary of the payment transaction. Using the nomenclature of Gifford, the challenge response in Linehan is a question for which the payment computer already knows the answer; the buyer answers the question and signs the answer, and the buyer's computer then combines the

signed answer with the payment order and sends it on to the payment computer. In other words, Linehan does not teach to sign the payment order, but to send a signed answer together with the *unsigned* payment order.

This distinction is important because having the buyer view and sign a summary of the transaction, as recited in the present claims, eliminates the possibility of approval forgery by way of "a man in the middle attack" in which an attacker is able to read and modify all messages between the buyer and the authentication service.

Further, regarding dependent claims 40, 47, and 54, Applicants respectfully submit that the databases described in Gifford fail to teach or suggest each feature described in the claims. Specifically, the claims describe sending a buyer profile to the buyer over a network, the buyer profile including a plurality of payment instruments and a plurality of shipping address.

Gifford discloses a plurality of databases, including an account database 73 (Gifford col. 8, line 3) and an authorized address database 75 (Gifford col. 8, line 4). Account database 73 maintains temporal spending amounts, such as the amount spent in the current day, and also maintains temporal spending limits (Gifford col. 8, lines 12-15). The account database may also maintain a translation between principal identifiers and external account identifiers (Gifford col. 8, lines 15-17). Address database 75 maintains for each sender a list of authorized buyer computer and delivery addresses (Gifford col. 8, lines 20-22).

Payment information, including an account number, are entered by a buyer in response to a requested purchase HTML form (*see* account number text entry box 13 in FIG. 4 and Gifford col. 5, lines 33-46). If the account number is not in the external financial system, it is translated into a corresponding account number in the external financial system using account database 73. The client computer address and the delivery address specified in the payment order are checked against the address database 75 by the payment computer (*see* Gifford col. 8, lines 33-35). If the addresses in the payment order are not in the database, the payment computer sends a rejection message to the client computer (*see* Gifford col. 8, lines 37-39).

These teachings of Gifford suggest away from sending the buyer's profile to the buyer so that a selection can be received of one of the plurality of payment instruments and one of the plurality of shipping addresses. For example, Gifford uses the delivery address provided by the buyer for transaction verification; if Gifford provides the buyer a selection of valid addresses,

this verification function is completely undermined. The Examiner's supposition that "Before selecting the method of payment and address information, the buyer must first be provided with his profile" is not supported.

Further, regarding dependent claims 36, 43, and 50, Applicants submit that these claims are also not obvious at least as further limitations on the independent claims. The combination of Baltzley with Gifford and Linehan fails to overcome the deficiencies of Gifford and Linehan described above.

**Conclusion**

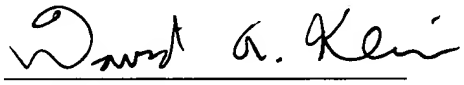
In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited.

Applicants authorize the Commissioner to charge any fees determined to be due with the exception of the issue fee and to credit any overpayment to Deposit Account No. 11-0600.

The Examiner is invited to contact the undersigned at (202) 220-4209 to discuss any matter concerning this application.

Respectfully submitted,
KENYON & KENYON

Dated: December 9, 2004



David A. Klein
Reg. No. 46,835

Kenyon & Kenyon
1500 K Street, N.W.
Suite 700
Washington, D.C. 20005
Tel: (202) 220-4200
Fax: (202) 220-4201

528595_1.DOC